



(51) International Patent Classification:
G08B 13/00 (2006.01) **G08B 31/00** (2006.01)
G06T 7/00 (2006.01)

(21) International Application Number:
PCT/MY2010/000147

(22) International Filing Date:
17 August 2010 (17.08.2010)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
PI 20093494 24 August 2009 (24.08.2009) MY

(71) Applicant (for all designated States except US): **MIMOS BERHAD** [MY/MY]; Technology Park of Malaysia, Bukit Jalil, 57000 Kuala Lumpur (MY).

(72) Inventors; and

(75) Inventors/Applicants (for US only): **LIANG, Kim Meng** [MY/MY]; c/o Mimos Berhad, Technology Park of Malaysia, Bukit Jalil, Kuala Lumpur 57000 (MY). **LIM, Mei Meng** [MY/MY]; c/o Mimos Berhad, Technology Park of Malaysia, Bukit Jalil, Kuala Lumpur 57000 (MY). **TANG, Sze Ling** [MY/MY]; c/o Mimos Berhad, Technology Park of Malaysia, Bukit Jalil, Kuala Lumpur 57000 (MY). **KADIM, Zulaikha** [MY/MY]; c/o Mimos Berhad, Technology Park of Malaysia, Bukit Jalil, Kuala Lumpur 57000 (MY).

(74) Agent: **MOHAN, K.**; Adastra Intellectual Property Sdn Bhd, A-28-10, Menara UOA Bangsar, No. 5, Jalan Bangsar Utama 1, 59000 Kuala Lumpur (MY).

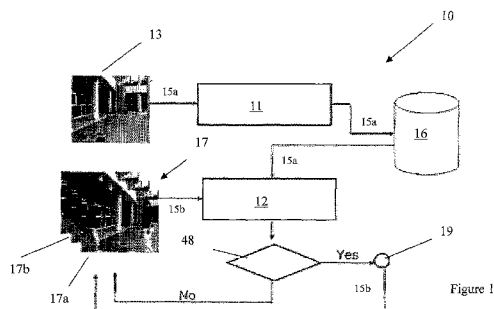
(81) Designated States (unless otherwise indicated, for every kind of national protection available): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PE, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Designated States (unless otherwise indicated, for every kind of regional protection available): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:

— with international search report (Art. 21(3))

(54) Title: SYSTEM AND METHOD TO DETERMINE SUSPICIOUS BEHAVIOR



(57) Abstract: A security system (10) for detecting suspicious event comprises an area selection module (11) and an analysis module (12). The area selection module (11) is used to specify (20) at least one suspicious boundary area (14) in a scene (13). The analysis module (12) then identify human in an image (17a) of the scene (13) whereby the identified human is analyzed to obtain gaze behavior information and the gaze behavior information is processed with predetermined rules to detect suspicious behavior event.



System and Method to Determine Suspicious Behavior

Field of Invention

The present invention relates generally to a security system, more particularly to a security system to determine suspicious behavior event using gaze analysis and the method thereof.

Background of the Invention

With the increase of the installation of capturing means such as optical camera in the room, building, airport, city and etc, monitoring task on the captured scene from each capturing means has become a major problem to the security industry. In the current security practices, the monitoring is carried out manually and usually involves security personnel in visually observing the potential intruder. Although the manual monitoring is the most effective choice based on the fact that human vision is powerful, but the level of effectiveness is decreases as the attention span and the number of monitor screen increases.

As described in US2006/0072010A1 and US2008/0193010A1, the human activity is been monitored based on position, direction, change of human geometry information, magnitude velocity and posture information of the human. Although the above extracted features are relevant to be analyzed for estimation of human activity in the scene, the particular scene on the capturing means are only triggered after the suspicious event had taken place. For example, a human with high velocity movement while performing fighting posture will actually trigger the system to indicate the event had happened. However, an effective

monitoring system should have the capability to assist security personnel to highlight the scene view before any suspicious event happens.

In the descriptions found in US2008/0221730A1, interaction of humans in the scene is analysed by determining the position and direction among humans in the scene. In another embodiment in US2007/0014439A1, a control monitoring system is described, which the direction and angle of an individual towards a specific object is analysed. The control monitoring system is used specifically for car theft scenario where the specific object is a vehicle. However, the proposed approach is not suitable for surveillance system in general, where complete analysis of the gaze information of individuals that interact in the scene is needed.

Thus, it would be desirable to provide an automated monitoring system to assist the security personnel to carry out the video monitoring task and to alert the security personnel before the suspicious event happens.

The objective of the present invention is to provide a suspicious behavior monitoring system based on gaze analysis.

Other objectives of this invention will become apparent on the reading of this entire disclosure.

Summary of the Invention

A system and analysis method based on gaze analysis in detecting suspicious behavior of individuals in the scene is presented. The analysis on the gaze information is effective to determine the suspicious level in the scene before the actual suspicious event happens. It is noted that the early suspicious level can be detected based on the frequency rate, distribution, location and association of the gaze information of individuals in the scene.

The suspicious behavior analysis system consists of two modules namely suspicious area selection module and behavior analysis module. The suspicious area selection module allows the suspicious boundary area with suspicious level to be determined. In behavior analysis model, individuals are tracked continuously in the scene and relevant information from each tracked individual is extracted, simultaneously. The extracted information is the direction of the tracked path, line of sight, area of sight and point of interest. The extracted information from individuals are analyzed in the behavior rule analysis process that contains the rule analysis steps which analyses on the frequency rate, distribution, location and association of the gaze information.

Brief Description of the Drawings

Other objects, features, and advantages of the invention will be apparent from the following description when read with reference to the accompanying drawings. In the drawings, wherein like reference numerals denote corresponding parts throughout the several views:

Figure 1 shows an overall architecture of a security system for detecting suspicious behavior event according to the present invention;

Figure 2 is a block diagram of the working mechanism of suspicious area selection module;

Figure 3 shows a diagram of the defined suspicious boundary area with selection of suspicious levels;

Figure 4 depicts a block diagram of the working mechanism of behavior analysis module;

Figure 5 is an illustration image of processes in behavior analysis module;

Figure 6 illustrates a flow chart of the seven rule analysis processes in behavior rule analysis module;

Figure 7 is a flow chart showing the steps performed in the first rule analysis;

Figure 8 is a flow chart showing the steps performed in the second rule analysis;

Figure 9 is a flow chart showing the steps performed in the third rule analysis;

Figure 10 is a flow chart showing the steps performed in the fourth rule analysis;

Figure 11 is a flow chart showing the steps performed in the fifth rule analysis;

Figure 12 is a flow chart showing the steps performed in the sixth rule analysis; and

Figure 13 is a flow chart showing the steps performed in the seventh rule analysis.

Detailed Description of the Preferred Embodiments

In the following detailed description, numerous specific details are set forth in order to provide a thorough understanding of the invention. However, it will be understood by those of ordinary skill in the art that the invention may be practiced without these specific details. In other instances, well-known methods, procedures and/or components have not been described in detail so as not to obscure the invention. Reference will now be made in detail to the preferred embodiments of the present invention, examples of which are illustrated in the accompanying drawings.

Figure 1 is an overview of an embodiment of a system (10) for detecting suspicious behavior according to the present invention for use by a user. The system (10) is in communication with a display unit (not shown) and a capturing means (not shown), wherein the system (10) is using gaze analysis to detect suspicious behavior of individuals. The system (10) comprises of a suspicious area selection module (11) and a behavior analysis module (12) as shown in Figure 1.

The suspicious area selection module (11) allows the user to specify (20) a suspicious boundary area (14) on a background image (13) captured by the capturing means and shown at the display unit. The suspicious area selection module (11) is performed in an offline mode as shown with arrows (15a) in Figure 1. The background image (13) is defined as a scene in

the image that does not contain any analyzed objects in the scene. The specified suspicious boundary areas (14) for the system (10) is contained in a suspicious area map and stored in a memory means (16), such as database.

In the process of specifying (20) the suspicious boundary area (14), user needs to determine (21) the type of geometric shape for the suspicious boundary area (14) as shown in Figure 2. The type of geometric shapes could be oval, circle, square, rectangle, upright triangle, downright triangle and other available shapes. User may then define (22) the suspicious boundary area (14) on the displayed scene background image (13) with the selected geometric shape from step (21). At least one suspicious boundary area (14) is defined (22) on the image (13). A suspicious level for each defined suspicious boundary area (14) is then selected (23) from either high or low level as shown in Figure 3. If more than one (24) suspicious boundary area (14) appears in the displayed scene background image (13), steps (21), (22) and (23) are repeated.

In the behavior analysis module (12), each sample from an image sequence (17) is processed (18) in order to determine (48) whether the scene in the sample of image contains suspicious events as shown in Figure 1. The image sequence (17) is obtained from the capturing means and the behavior analysis module (12) is performed in an online mode as shown with arrows (15b) in Figure 1. If a suspicious event is detected, an alert (19) will be triggered. This module (12) automatically predicts the suspicious events for each scene image that happen in the scene.

In the step of processing (18) each image (17a) from the image sequence (17), the processes include the operations of motion detection (30), human detection (31) and human tracking

(32). After the tracked human is processed, the step of processing (18) will further perform the operations of path direction estimation (33), line-of-sight direction detection (34), point-of-interest detection (35), area-of-sight detection (36) and behavior rule analysis (37) as shown in Figures 4 and 5.

In the motion detection (30) operation, the areas in the image (17a) that contains moving objects are determined by tracking the intensity difference between two images (17a, 17b) in sequence order from the image sequence (17). The moving areas in the image (17a) will serve as the focus area to be analyzed in the following processes or operations. In the human detection (31) operation, the valid moving areas to be analyzed are determined for behavior analysis. The valid moving area of focus contains human, where the pattern of the intensities in the moving area is compared with the pattern of intensities that resembles human. In the human tracking (32) operation, for each human, the location of the particular human along the image sequence (17) is tracked. The particular human will be assigned with a consistent label (38) throughout the image sequence (17).

The tracked human is then further processed with path direction estimation (33) operation where the direction is calculated from the temporal information of the location of the tracked human. The gaze direction for each tracked human is then determined by analyzing the position of the head, body, foot and et cetera in the line-of-sight direction detection (34) operation. Then the point of interest of the scene is determined by analyzing the intersection location of more than one line of sight from the tracked humans in the point-of-interest detection (35) operation. This point of interest highlights specific location in the image (17a) that humans are frequently observing. Then in the area-of-sight detection (36) operation, the

common sight area from the tracked humans is determined, where the common sight area highlights the region in the image (17a) that the majority of the humans are observing.

The outputs from operations after the operation of human is tracked, are stored in a memory means (39) as gaze information. Then the behavior rule analysis (37) operation is performed with specific defined rules on the retrieved gaze information from the memory means (39) to determine the occurrence of suspicious event. In this operation (37), a plurality of rule analysis processes is performed. In a preferred embodiment of the present invention, the behavior rule analysis (37) operation is preferably having seven processes namely a first rule analysis (40), second rule analysis (41), third rule analysis (42), fourth rule analysis (43), fifth rule analysis (44), sixth rule analysis (45) and seventh rule analysis (46) as shown in Figure 6. However, it should be understood that the invention is not limited to these seven rule analysis processes described herein. Instead, any combination or sequence of the following processes is contemplated to implement the invention. Therefore other possible solutions and processes may be added to the present invention to determine the suspicious event.

The behavior rule analysis (37) operation starts from the first rule analysis (40) to determine (64) the suspicious event. If the suspicious event is detected (65), an alert is triggered (67). If suspicious event is not detected (66), the rule analysis process continues through the rule analysis process until the seventh rule analysis (46).

The first rule analysis (40) is used to analyse the line-of-sight with the path direction for determining suspicious event as shown in Figure 7. This is based on the fact that human tend to look at the direction in which he/she is heading towards although there may be deviations at some point of time. Deviations that exceed a threshold time span reflects suspicious

behavior and the threshold value may differ from one application to another depending on the severity of the system (10). In a preferred embodiment, the first rule analysis (40) includes four steps to determine the suspicious event. In a first step, a deviation of line-of-sight of a tracked human from its own path direction is determined (50) if the deviation is equal or more than a threshold degree as shown in Figure 7. In the present invention, the threshold degree is recommended equivalent to 90.

The total number of detected deviation of line-of-sight from path direction (51) and the frequency percentage of deviation of line-of-sight from path direction (52) are then computed. The frequency percentage is calculated with Equation 1 as follows:

$$\text{Frequency Percentage} = \frac{\text{Total deviation of line - of - sight from path direction}}{\text{Total number of processed image}} \times 100 \dots\dots\dots (1)$$

The computed frequency percentage is then compared (53) with the predetermined threshold for first rule analysis (40). If the computed frequency is above (53a) the threshold, the suspicious event is detected. If otherwise (53b), the normal event is detected.

The second rule analysis (41) is used to analyse the line-of-sight with the area-of-sight for determining suspicious event as shown in Figure 8. This is based on the assumption that in a particular scene where there is no predetermined suspicious boundary area, a subject whose line-of-sight differ from the common line-of-sights of other subjects in the scene which is represented by the area-of-sight in this invention should be categorized as suspicious. In a preferred embodiment, the second rule analysis (41) includes four steps to determine the suspicious event. In a first step, a deviation of line-of-sight of a tracked human from the available area-of-sight is determined (60) if the deviation is more than a predetermined

distance. The predetermined distance is determined base on the severity of the security consideration in the scene.

The total number of detected deviation of line-of-sight from available area-of-sight (61) and the frequency percentage of deviation of line-of-sight from available area-of-sight (62) are computed. The frequency percentage is calculated with Equation 2 as follows:

$$\text{Frequency Percentage} = \frac{\text{Total deviation of line - of - sight from area - of - sight}}{\text{Total number of processed image}} \times 100 \dots\dots\dots (2)$$

The computed frequency is then compared (63) with the predetermined threshold for second rule analysis (41). If the computed frequency is above (63a) the threshold, the suspicious event is detected. If otherwise (63b), the normal event is detected.

The third rule analysis (42) is used to analyse the line-of-sight with the predefined suspicious boundary area (14) for determining suspicious event as shown in Figure 9. In a preferred embodiment, the third rule analysis (41) includes four steps to determine the suspicious event. In a first step, an intersection of line-of-sight on suspicious boundary area (14) is calculated (70). The total number of detected intersections between line-of-sight and the suspicious boundary area (14) is then computed (71), which reflects that a human subject is observing the particular predetermined suspicious area. The frequency percentage of intersection between line-of-sight and the suspicious boundary area is also computed (72). The frequency percentage is calculated with Equation 3 as follows.

$$\text{Frequency Percentage} = \frac{\text{Total int er sec tion between line - of - sight and suspicious boundary area}}{\text{Total number of processed image}} \times 100 \dots\dots\dots (3)$$

The computed frequency is then compared (73) with the predetermined threshold for third rule analysis (42). If the computed frequency is above (73a) the threshold, the suspicious event is detected. If otherwise (73b), the normal event is detected.

The fourth rule analysis (43) is used to analyse the point-of-interest with the predefined suspicious boundary area (14) for determining suspicious event as shown in Figure 10. In a preferred embodiment, the fourth rule analysis (43) includes four steps to determine the suspicious event. In a first step, an intersection between the detected point-of-interest and suspicious boundary area (14) is calculated (80). Similar to the third rule analysis (42), this rule (43) aims to trigger an alert when the number of observers on a predetermined suspicious area is above a threshold value. The only distinction between the fourth rule analysis (43) and third rule analysis (42) is the latter analyses the line-of-sight of a single subject whereas the former analyses on the point of interest; point of interest is the result of an analysis of more than one line-of-sights.

The total number of detected deviation of point-of-interest (81) on suspicious boundary area (14) and the frequency percentage of intersection of point-of-interest (82) on suspicious boundary area (14) are then computed. The frequency percentage is calculated with Equation 4 as follows:

$$\text{Frequency Percentage} = \frac{\text{Total intersection between point-of-interest and suspicious boundary area}}{\text{Total number of processed image}} \times 100$$

..... (4)

The computed frequency is then compared (83) with the predetermined threshold for fourth rule analysis (43). If the computed frequency is above (83a) the threshold, the suspicious event is detected. If otherwise (83b), the normal event is detected.

The fifth rule analysis (44) is used to analyse the changes of point-of-interest in the scene for determining suspicious event as shown in Figure 11. The fifth rule analysis (44) assumes that there is no predetermined suspicious boundary area and that the consistency of a particular point in the scene to be detected as the point-of-interest by the system (10) reflects the suspiciousness. In a preferred embodiment, the fifth rule analysis (44) includes three steps to determine the suspicious event. In a first step, the total number of consistent point-of-interest throughout the image sequence is calculated (90). The point-of-interest is considered to be consistent if the point-of-interest appears throughout the image sequence or point-of-interest continuously reappears at the same location in the scene. The frequency percentage of consistent point-of-interest (91) is then computed. The frequency percentage is calculated with Equation 5 as follows:

$$\text{Frequency Percentage} = \frac{\text{Total consistent point-of-interest}}{\text{Total number of processed image}} \times 100 \dots\dots\dots (5)$$

The computed frequency is then compared (92) with the predetermined threshold for fifth rule analysis (44). If the computed frequency is above (92a) the threshold, the suspicious event is detected. If otherwise (92b), the normal event is detected.

The sixth rule analysis (45) is used to analyse the changes of the direction of line-of-sight in the scene for determining suspicious event as shown in Figure 12. This rule allows detection of a particular subject having a focus on a particular location for a period of time. In a preferred embodiment, the sixth rule analysis (44) includes three steps to determine the suspicious event. In a first step, the total number of consistent line-of-sight throughout the image sequence is calculated (100). The line-of-sight is considered to be consistent if the line-of-sight of the tracked human throughout the image sequence is almost at the similar

direction. The frequency percentage of consistent line-of-sight (101) is then computed. The frequency percentage is calculated with Equation 6 as follows:

$$\text{Frequency Percentage} = \frac{\text{Total consistent line - of - sight}}{\text{Total number of processed image}} \times 100 \dots\dots\dots (6)$$

The computed frequency is then compared (102) with the predetermined threshold for sixth rule analysis (45). If the computed frequency is above (102a) the threshold, the suspicious event is detected. If otherwise (102b), the normal event is detected.

The seventh rule analysis (46) is used to analyse the changes of the direction of line-of-sight in the scene for determining suspicious event as shown in Figure 13. The seventh rule analysis (46) considers that a subject whose line-of-sight changes frequently from one point to another as suspicious. This is based on the fact that a curious person would not have a determined path and focus but instead would have a distracted line-of-sight. For an instance, a criminal who observe the environment for CCTV before committing a crime may have a random line-of-sight over a period of time.

In a preferred embodiment, the seventh rule analysis (46) includes three steps to determine the suspicious event. In a first step, the total number of random line-of-sight throughout the image sequence is calculated (110). The line-of-sight is considered to be random if the line-of-sight of the tracked human throughout the image sequence changes randomly in terms of direction. The frequency percentage of random line-of-sight (111) is then computed. The frequency percentage is calculated with Equation 7 as follows.

$$\text{Frequency Percentage} = \frac{\text{Total random line - of - sight}}{\text{Total number of processed image}} \times 100 \dots\dots\dots (7)$$

The computed frequency is then compared (112) with the predetermined threshold for seventh rule analysis (46). If the computed frequency is above (112a) the threshold, the suspicious event is detected. If otherwise (112b), the normal event is detected.

If none of the suspicious event detected throughout the seven rule analysis processes, then the analyzed scene image is having normal event and no alert is triggered.

As will be readily apparent to those skilled in the art, the present invention may easily be produced in other specific forms without departing from its essential characteristics. The present embodiments is, therefore, to be considered as merely illustrative and not restrictive, the scope of the invention being indicated by the claims rather than the foregoing description, and all changes which come within therefore intended to be embraced therein.

Claims

1. A security system (10) for detecting suspicious event comprising:
an area selection module (11) which is used to specify (20) at least one suspicious boundary area (14) in a scene (13); and
an analysis module (12) that identify human in an image (17a) of said scene (13) whereby said identified human is analyzed to obtain gaze behavior information and said gaze behavior information is processed (37) with predetermined rules to detect suspicious behavior event.
2. The security system (10) for detecting suspicious event as claimed in claim 1, wherein said area selection module (11) is a suspicious area selection module which is performed in an offline mode (15a).
3. The security system (10) for detecting suspicious event as claimed in claim 2, wherein said suspicious area selection module (11) allows user to determine (21) the type of geometric shape and to define (23) the level of suspicious for said suspicious boundary area (14).
4. The security system (10) for detecting suspicious event as claimed in claim 1, wherein said analysis module (12) is a behavior analysis module (12) which is performed in an online mode (15b).
5. The security system (10) for detecting suspicious event as claimed in claim 4, wherein said behavior analysis module (12) in identifying human in said image (17a) includes any or in combination of the operations of motion detection (30), human detection (31) and human tracking (32).

6. The security system (10) for detecting suspicious event as claimed in claim 4, wherein said motion detection (30) operation of said behavior analysis module (12) determines areas in said image (17a) that contains moving objects by tracking the intensity difference between two images (17a, 17b) from the image sequence (17).

7. The security system (10) for detecting suspicious event as claimed in claim 4, wherein said human detection (31) operation of said behavior analysis module (12) determines moving area contains human by comparing the pattern of the intensities in said moving area with the pattern of intensities that resembles human.

8. The security system (10) for detecting suspicious event as claimed in claim 4, wherein said human tracking (32) operation of said behavior analysis module (12) tracks the location of each particular human along the image sequence (17) and said each particular human will be assigned with a consistent label (38) throughout the image sequence.

9. The security system (10) for detecting suspicious event as claimed in claim 1, wherein said gaze behavior information includes path direction (33), line of sight (34), area of sight (36) and point of interest (35).

10. A method for detecting suspicious event, said method comprising the steps of:
specifying (20) at least one suspicious boundary area (14) in a scene (13); and
analyzing an image (17a) of said scene (13) to detect suspicious behavior event, said step of analyzing comprising the steps of:
identifying human in said image (17a);
obtaining gaze behavior information by analyzing said identified human; and

processing said gaze behavior information with predetermined rules to detect suspicious behavior event.

11. The method for detecting suspicious event as claimed in claim 10, wherein said step of specifying (20) said boundary area (14) includes steps of defining (21) the type of geometric shape for said boundary area (14) and defining (23) the suspicious level for said defined boundary area (14).

12. The method for detecting suspicious event as claimed in claim 10, wherein said step of identifying human includes of motion detecting (30), human detecting (31) and human tracking (32).

13. The method for detecting suspicious event as claimed in claim 10, wherein said step of obtaining gaze behavior information includes the steps of:

estimating (33) the path direction for each identified human by calculating from the temporal information of the location of said identified human;

detecting (34) the line-of-sight direction by analyzing the position of the head, body and foot;

determining (35) the point of interest by analyzing the intersection location of more than one line of sight from the identified human; and

determining (36) the area of sight where the common sight are from said identified human is determined.

14. The method for detecting suspicious event as claimed in claim 10, wherein said step of processing said gaze behavior information includes seven predetermined rules which are the first rule analysis (40) to analyse the line of sight with the path direction, second rule analysis

(41) to analyse the line of sight with the area of sight, third rule analysis (42) to analyse the line of sight with the predefined suspicious boundary area (14), fourth rule analysis (43) to analyse the point of interest with the predefined suspicious boundary area (14), fifth rule analysis (44) to analyse the changes of point-of-interest in the scene, sixth rule analysis (45) to analyse the changes of the direction of line-of-sight in the scene, and seventh rule analysis (46) to analyse the changes of the direction of line-of-sight in the scene.

15. The method for detecting suspicious event as claimed in claim 14, wherein said in each rule analysis, if the suspicious event is detected (65), an alert is triggered (67) and if suspicious event is not detected (66), the rule analysis process continues through the rule analysis process until the seventh rule analysis (46).

1/8

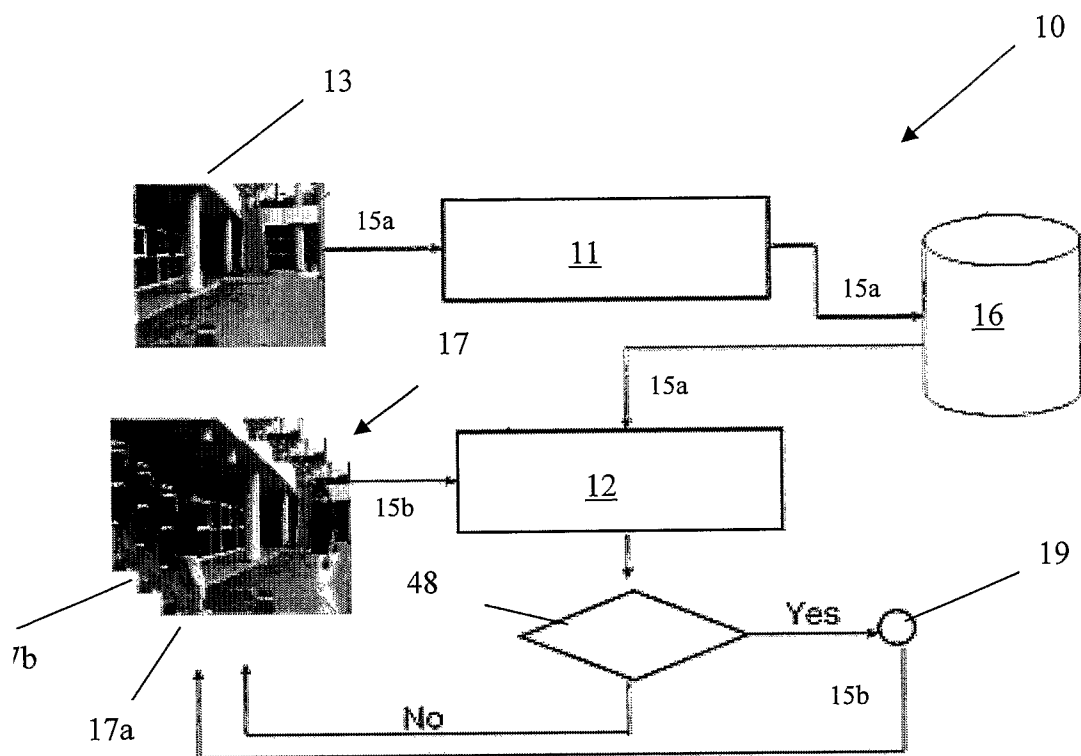


Figure 1

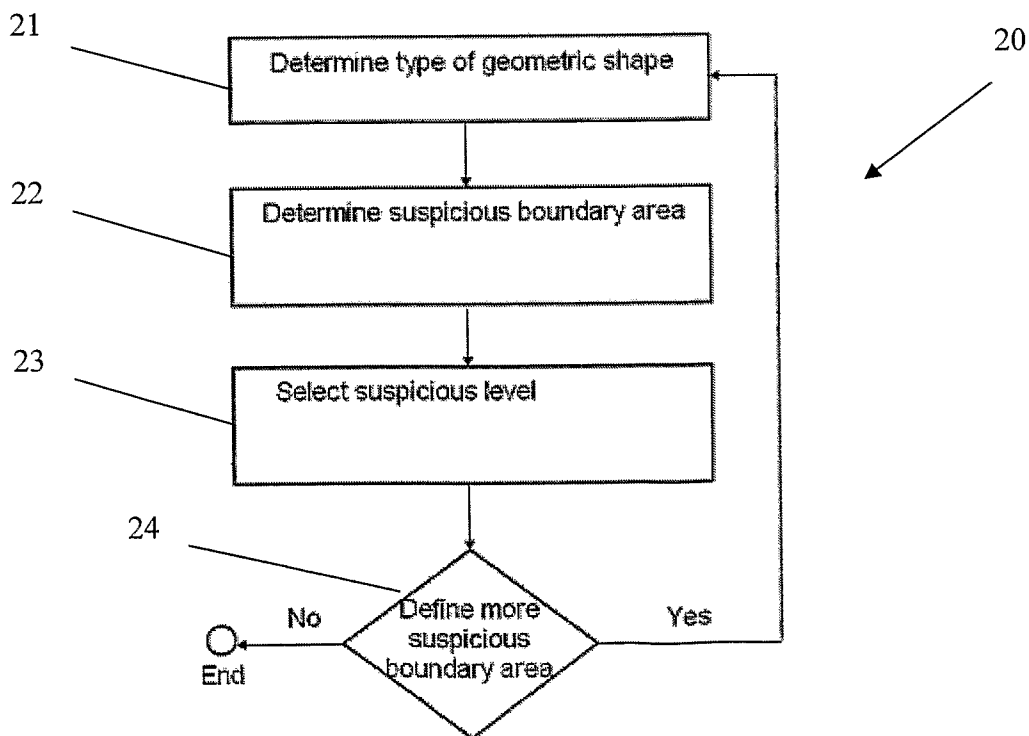


Figure 2

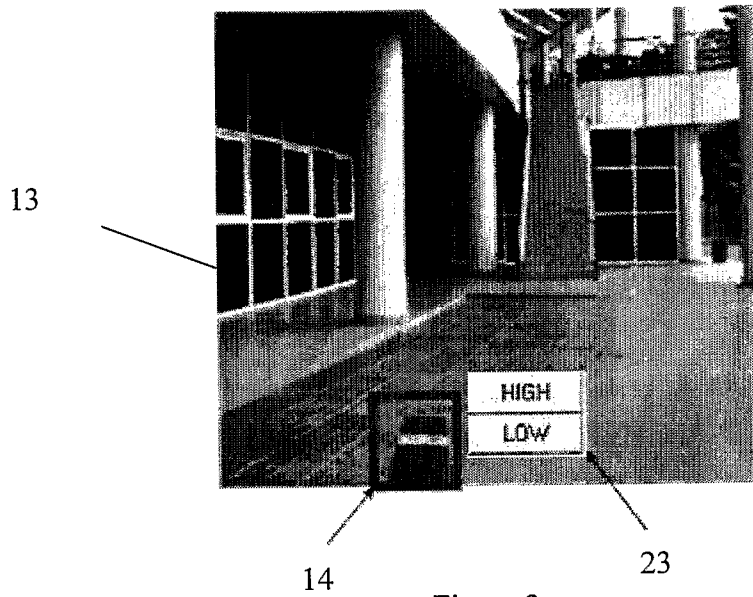


Figure 3

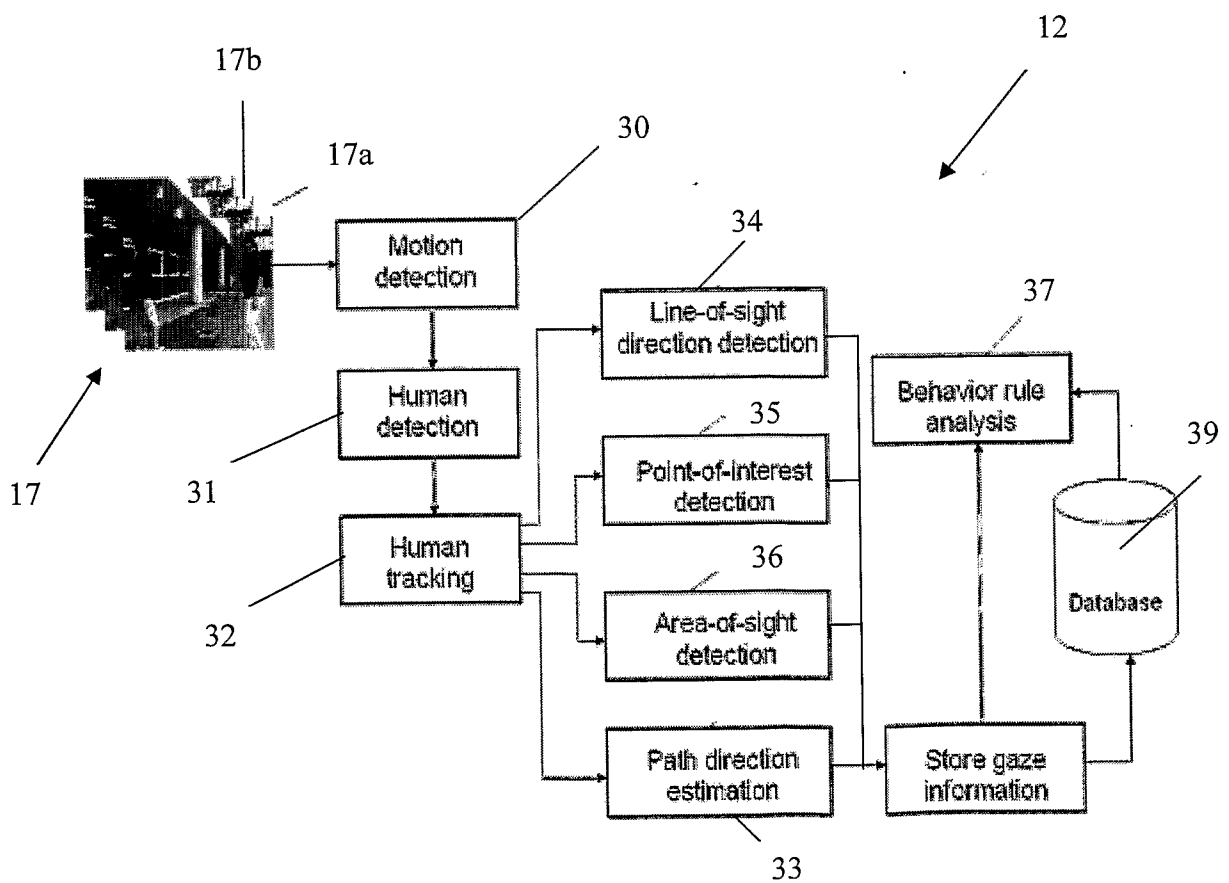


Figure 4

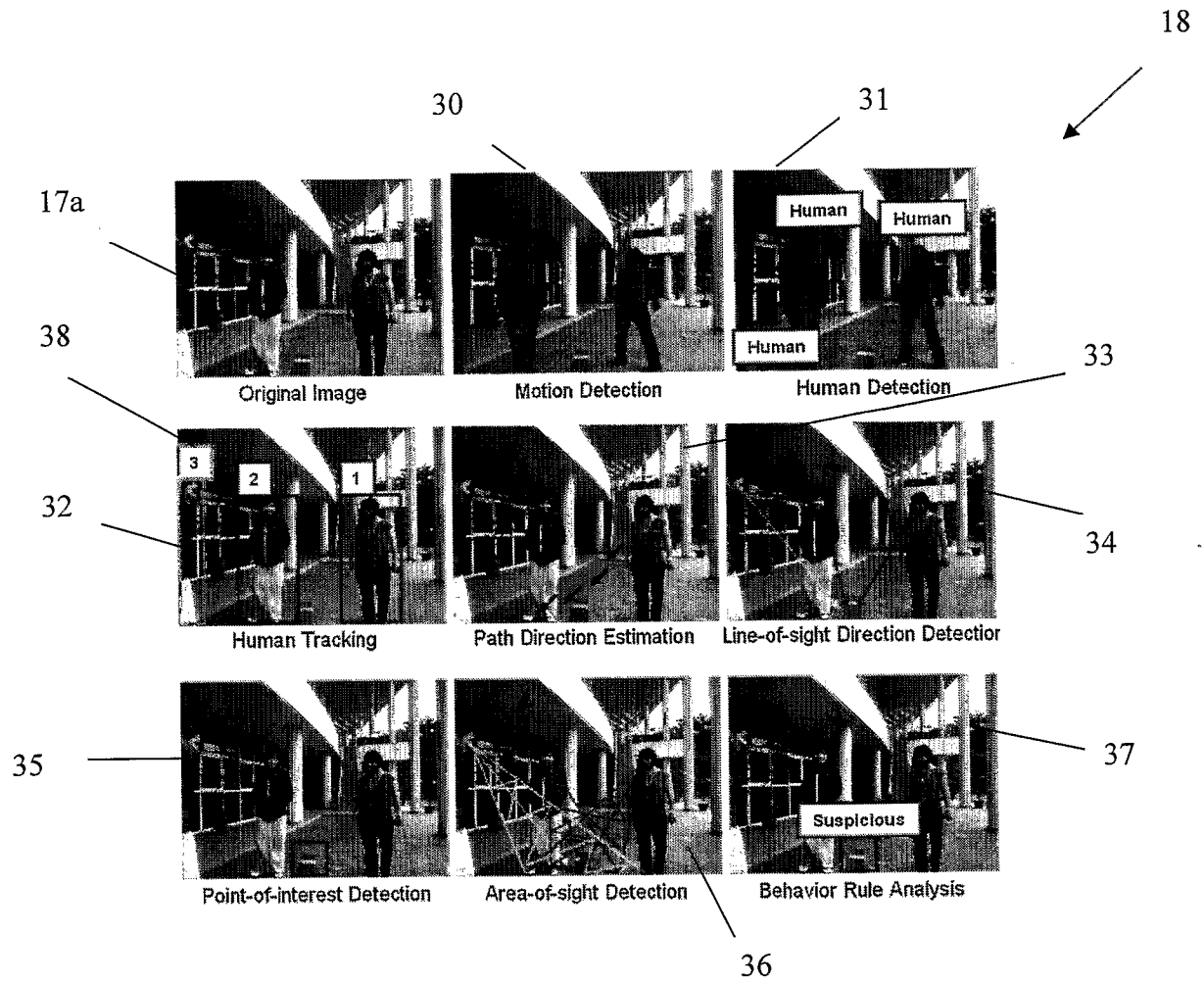


Figure 5

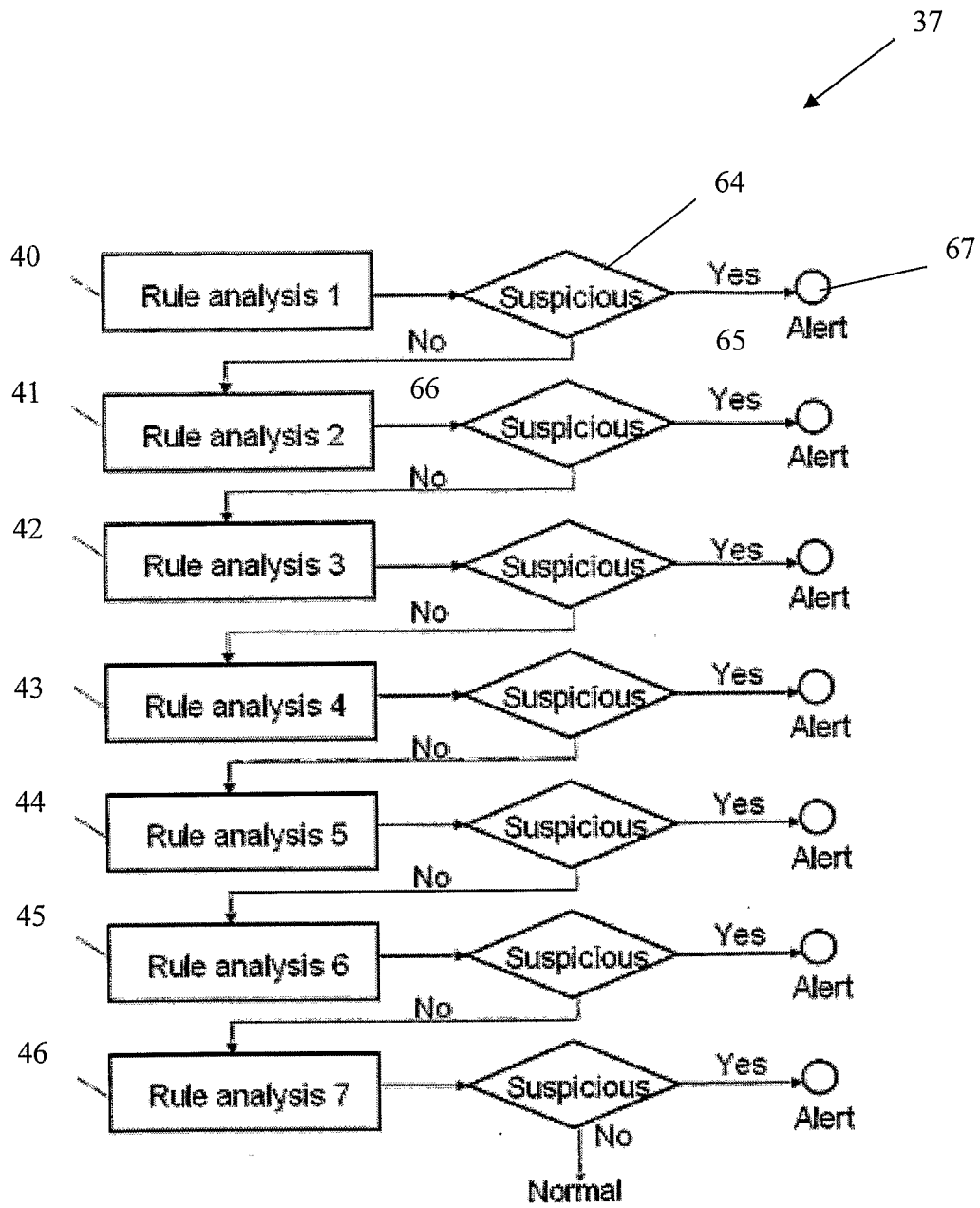


Figure 6

5/8

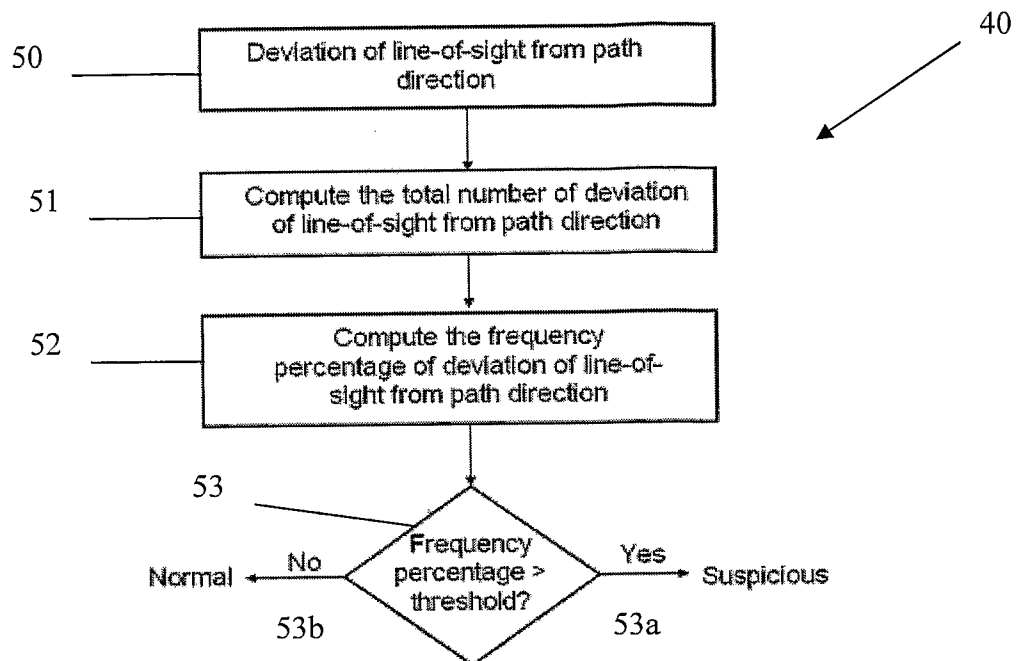


Figure 7

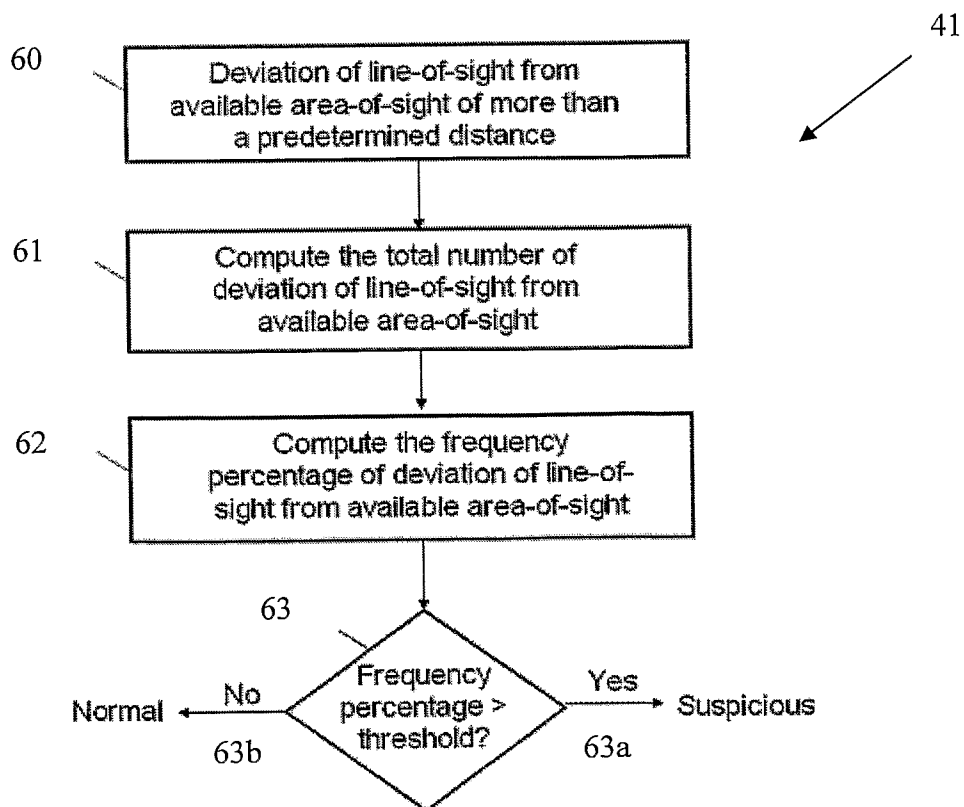


Figure 8

6/8

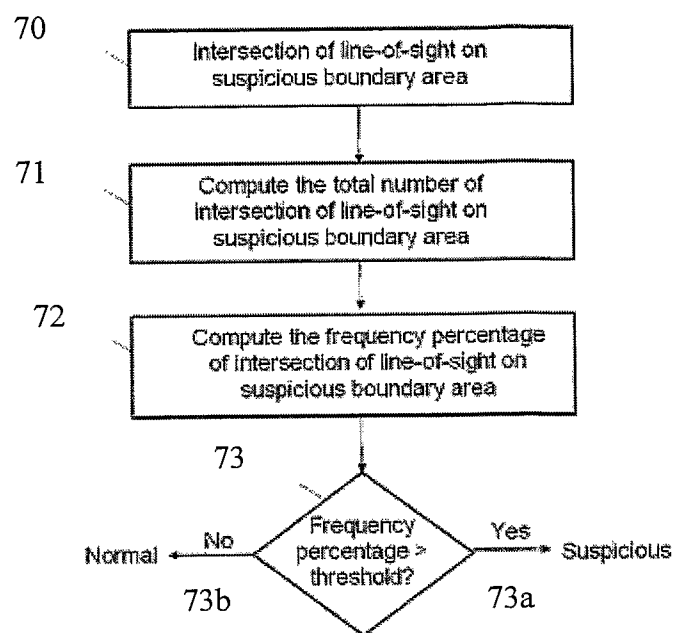


Figure 9

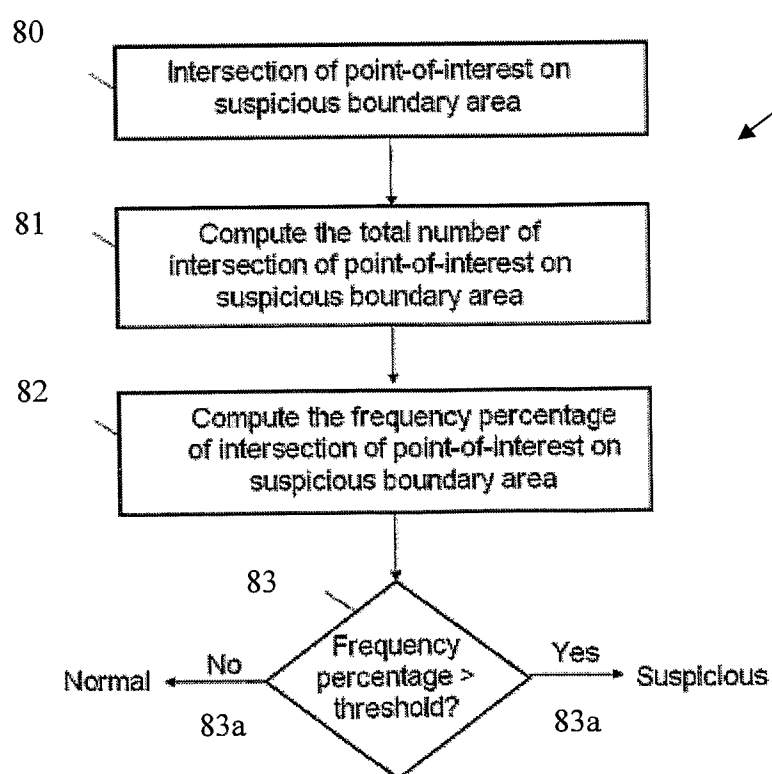


Figure 10

7/8

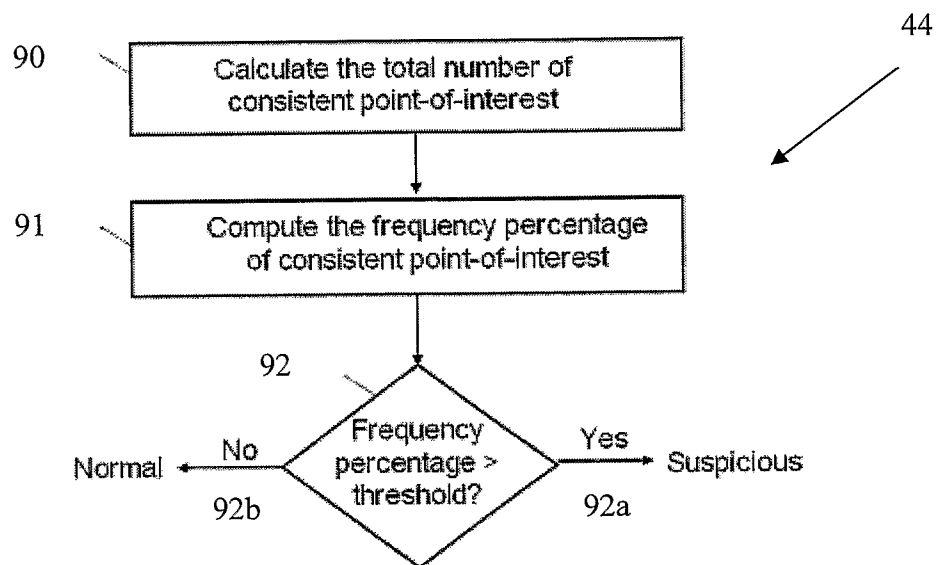


Figure 11

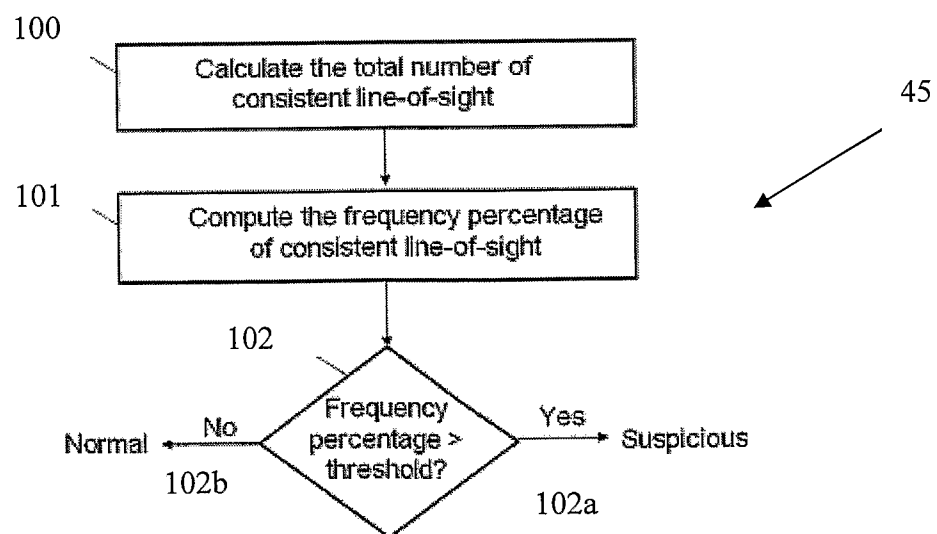


Figure 12

8/8

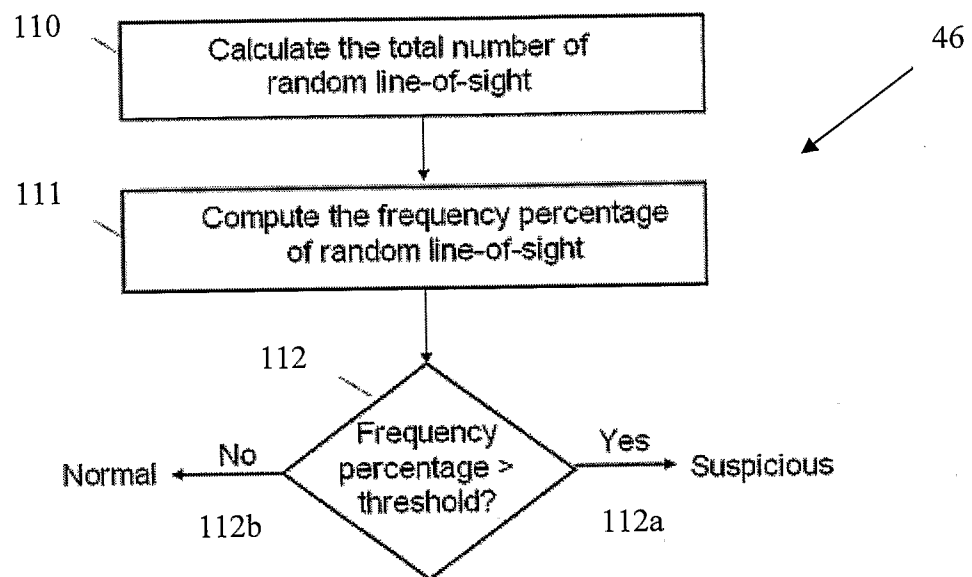


Figure 13

INTERNATIONAL SEARCH REPORT

International application No.
PCT/MY2010/000147**A. CLASSIFICATION OF SUBJECT MATTER**Int. Cl. **G08B 13/00** (2006.01) **G06T 7/00** (2006.01) **G08B 31/00** (2006.01)

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

WPI, Google Patents, Patentscope, internet "gaze, face, direction surveillance etc."

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	N. M. ROBERTSON et al., "Automatic Human Behaviour Recognition and Explanation for CCTV Video Surveillance", Security Journal, 2006. Chapters 1 to 5 in particular.	1-5,10-13
Y	In view of "Multiple Object Tracking in Real-Time" below.	6-8
Y	In view of "Head Orientation and Gaze Direction in Meetings" below.	9
X	US 2007/0014439 A1 (ANDO) 18 January 2007 Paragraphs 168, 274 and 425 to 435 in particular.	1-15
X	US 7460150 B1 (COUGHLAN et al.) 2 December 2008 Column 3 to line 33 to column 8 line 26 in particular.	1-5,9-13
Y	In view of "Multiple Object Tracking in Real-Time" below.	6-8
Y	D. R. CORBETT, "Multiple Object Tracking in Real-Time", Thesis (Master), The University of Queensland, Brisbane, Australia, 2000. Page 12 (chapter 3.2) and page 44 in particular.	6-8
Y	R. STIEFELHAGEN et al., "Head Orientation and Gaze Direction in Meetings", Proceedings of ACM CHI, Minneapolis: ACM 2002. Paragraphs under "Introduction" and "Data Collection" in particular.	9



Further documents are listed in the continuation of Box C



See patent family annex

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"E" earlier application or patent but published on or after the international filing date

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"O" document referring to an oral disclosure, use, exhibition or other means

"&" document member of the same patent family

"P" document published prior to the international filing date but later than the priority date claimed

Date of the actual completion of the international search

18 November 2010

Date of mailing of the international search report

23 NOV 2010

Name and mailing address of the ISA/AU

AUSTRALIAN PATENT OFFICE
PO BOX 200, WODEN ACT 2606, AUSTRALIA
E-mail address: pct@ipaustralia.gov.au
Facsimile No: +61 2 6283 7999

Authorized officer

P. THONG
AUSTRALIAN PATENT OFFICE
(ISO 9001 Quality Certified Service)
Telephone No : +61 2 6283 2128

INTERNATIONAL SEARCH REPORT,

Information on patent family members

International application No.

PCT/MY2010/000147

This Annex lists the known "A" publication level patent family members relating to the patent documents cited in the above-mentioned international search report. The Australian Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

Patent Document Cited in Search Report				Patent Family Member	
US	2007/0014439	EP	1703437	JP	2006259828
US	7460150	NONE			
Due to data integration issues this family listing may not include 10 digit Australian applications filed since May 2001.					
END OF ANNEX					